What is claimed is:

1. A method of generating a key for encryption or decryption of data comprising:

a) generating parameters for a digital light interference signal generator;

b) using said digital light interference signal generator to generate a series of luminance measurements at an interference fringe;

c) converting said measurements into a series of numbers; and

d) generating a key for encryption or decryption of data based on said series of numbers.

2. A method of generating a key for encryption or decryption of data comprising:

a) generating parameters for a two optical signals;

b) using a light interference measuring device to generate a series of luminance measurements at an interference fringe of said two optical signals;

c) converting said measurements into a series of numbers; and

d) generating a key for encryption or decryption of data based on said series of numbers.

3. A cryptographic system comprising:

1) software or hardware for segmenting and converting a cryptograph key into two digital optical signals with amplitudes,

wavelengths, and initial phases, and an initial aberration (optical path length difference) at a point P where the two digital optical signals meet;

2) software or hardware for encrypting and decrypting using a digital light interference signal generator used to dynamically generate aberration value changes, with the luminance of a light interference fringe at point P changing as the aberration changes generating a series of random numbers;

3) software or hardware for using the series generating a ciphertext by XOR operations between the plaintext and the random numbers generated by the digital light interference signal generator;

4. The system of claim 3 wherein the ciphertext is also deciphered using a process similar to the encryption process, with the only difference being that the plaintext is recovered by XOR operations between the ciphertext and the random numbers.

5. The system of claim 3 wherein the cryptograph key is segmented and converted into amplitudes, wavelengths, initial phases, and initial aberration of digital optical signals comprising a means for adjusting the mathematical precision of the amplitudes, wavelengths, initial phases, and aberration to get the sequence of random numbers from the digital light interference signal generator.

6. The system of claim 3 wherein the method of encrypting or decrypting the data comprises the step of:

a) repeating until filling cryptograph key into a key buffer until the key is 128 bits long;

b) segmenting the key buffer into 32 bit sub keys;

c) converting the sub keys to amplitudes A, wavelengths λ, initial phases Φ_0, and initial aberration x_0 of a digital optical signal;

d) calculating an initial value y_0 to be used as an initial value of y_n as a feed back signal;

e) in order to generate an initial state of a light interference using equations $x_1 = A*\cos(\pi/\lambda*x_0)*\sin(\Phi_0)+y_0$ and $y_1=-x_0$;

f) in order to generate the sequential random numbers using equations $x_{n+1} = A*\cos(\pi/\lambda*x_n)*\sin(\Phi_0)+y_n$ and $y_{n+1}=-x_n$.